

Ισοϋπόλοιοι αριθμοί mod m

Ορισμός: Δύο ακέραιοι a, b ονομάζονται ισοϋπόλοιοι mod m $(\Leftrightarrow)$ διαβαλύνονται με το m, αφήνουν το ίδιο υπόλοιπο.

Τότε συμβολίζω $a \equiv b \pmod{m}$ Διαβάω: "α ισοϋπόλοιος mod m"

Παράδειγμα $v[9:4]=1$, $v[13:4]=1$

Άρα οι αριθμοί 13, 9 λείπουν ισοϋπόλοιοι mod 4.

Συμβολίζω: $13 \equiv 9 \pmod{4} (\Leftrightarrow) 9 \equiv 13 \pmod{4}$.

Αν θεωρήσω τη διαίρεση $a \overline{) 4}$ τα δυνατά υπόλοιπα είναι $v = 0, 1, 2, 3$.

$$a = 4k + v.$$

1^η Αν $a = 4k \Leftrightarrow a \equiv 0 \pmod{4}$

2^η Αν $a = 4k + 1 \Leftrightarrow a \equiv 1 \pmod{4}$, Αν $a = 4k + 2 \Leftrightarrow a \equiv 2 \pmod{4}$...

Θεώρημα: Αν $a \equiv b \pmod{m}$ τότε $m \mid a - b$. και αντίστροφα:

Αν $m \mid a - b$ τότε $a \equiv b \pmod{m}$.

Απόδειξη: $(\Rightarrow)$ Έχω $a \equiv b \pmod{m} \Leftrightarrow v[a:m] = v$, $v[b:m] = v$

$$\left. \begin{array}{l} a = k \cdot m + v \text{ με } 0 \leq v < m \\ b = \lambda m + v \text{ με } 0 \leq v < m \end{array} \right\}$$

$$a - b = km - \lambda m \Leftrightarrow a - b = m(k - \lambda) \Rightarrow a - b = n \cdot m \Leftrightarrow m \mid a - b.$$

$(\Leftarrow)$ Έχω $m \mid a - b$, έστω ότι το υπόλοιπο της διαίρεσης $b:m$ είναι $v \Rightarrow b = p \cdot m + v$, $0 \leq v < m$ Στόχος: θα δείξω ότι $v[a:m] = v$

Αφού $m \mid a - b \Rightarrow$ υπάρχει ακέραιος φ : $a - b = \varphi m \Leftrightarrow a = \varphi m + b$

$$\Leftrightarrow a = \varphi m + p m + v \Leftrightarrow a = m(\varphi + p) + v \Rightarrow a = m \cdot A + v \quad 0 \leq v < m$$

$\Rightarrow$ το v είναι το υπόλοιπο της διαίρεσης του a δια m

Άρα οι αριθμοί a, b είναι ισοϋπόλοιοι mod m.

Αντίστοιχοι εφαρμογές των παραπάνω θεωρημάτων

1) 17, 12. $17 - 12 = 5 \Rightarrow 5 \mid 17 - 12 \Leftrightarrow 17 \equiv 12 \pmod{5}$

2) 192, 92 $192 - 92 = 100$. $20 \mid 100 \Leftrightarrow 20 \mid 192 - 92 \Leftrightarrow 192 \equiv 92 \pmod{20}$

Θεώρημα

1) Αν $a \equiv b \pmod{m}$ τότε $b \equiv a \pmod{m}$

Αποδ. Αφού $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b \Leftrightarrow m \mid b - a \Leftrightarrow b \equiv a \pmod{m}$

2) Αν $a \equiv b \pmod{m}$ και $b \equiv \gamma \pmod{m}$ τότε $a \equiv \gamma \pmod{m}$.
[ονομάζονται μεταβατική ιδιότητα].

Αποδ. Αφού $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b$ $\Rightarrow m \mid a - b + b - \gamma \Rightarrow$
 $b \equiv \gamma \pmod{m} \Leftrightarrow m \mid b - \gamma$ $\Rightarrow m \mid a - \gamma \Leftrightarrow a \equiv \gamma \pmod{m}$

3) Αν $a \equiv b \pmod{m}$ τότε $a + \gamma \equiv b + \gamma \pmod{m}$

Αποδ. Αφού $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b \Leftrightarrow m \mid a + \gamma - \gamma - b \Leftrightarrow$
 $m \mid (a + \gamma) - (b + \gamma) \Leftrightarrow a + \gamma \equiv b + \gamma \pmod{m}$

4) Αν $a \equiv b \pmod{m}$ τότε $a \cdot \gamma \equiv b \cdot \gamma \pmod{m}$

Αποδ. Αφού $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b \Rightarrow m \mid (a - b) \cdot \gamma \Leftrightarrow m \mid a\gamma - b\gamma \Leftrightarrow a\gamma \equiv b\gamma \pmod{m}$.

Προσοχή: Δεν μπορούμε να διαίρεσουμε και να 2 μέλη μιας ισοϋπολογίας mod m με τον ίδιο αριθμό.

$$\begin{array}{r} 20 \overline{) 4} \\ 0 \overline{) 5} \end{array} \quad \begin{array}{r} 16 \overline{) 4} \\ 0 \overline{) 4} \end{array} \quad \text{Άρα } 20 \equiv 16 \pmod{4} \xrightarrow{:\cdot 2} 10 \equiv 8 \pmod{4} \Leftrightarrow$$

$$4 \mid 10 - 8 \Leftrightarrow$$

5) Αν $a \equiv b \pmod{m}$ και $\gamma \equiv \delta \pmod{m}$

$$4 \mid 2 \text{ άνω } 0.$$

Τότε $a + \gamma \equiv (b + \delta) \pmod{m}$

Αποδ. Αφού $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b$ $\Rightarrow m \mid a - b + \gamma - \delta \Leftrightarrow$
 $\gamma \equiv \delta \pmod{m} \Leftrightarrow m \mid \gamma - \delta$ $\Rightarrow m \mid (a + \gamma) - (b + \delta) \Leftrightarrow$
 $a + \gamma \equiv (b + \delta) \pmod{m}$

Αν $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, $a_3 \equiv b_3 \pmod{m}$...
 $(a_1 + a_2 + a_3 + \dots) \equiv (b_1 + b_2 + b_3 + \dots) \pmod{m}$

Αδελφίσματα:

1) Να αποδείξετε ότι $17 \mid 16^3 + 1$, $15 \mid 16^3 - 1$, $19 \mid 21^3 - 8$, $23 \mid 21^3 + 8$.

2) Να αποδείξετε ότι $13 \mid 14^5 - 1$

3) Να βρείτε τις ακέραιες ρίζες της εξίσωσης: $x^4 + x^3 - x - 1 = 0$